Advisory Alert

Alert Number: AAA20240618 **Date:** June 18, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Arbitrary Code Execution Vulnerability
F5	**High**	VPN TunnelVision Vulnerability
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2024-24787)
Description	IBM has released security updates addressing an Arbitrary Code Execution Vulnerability that exists in Golang Go caused due to a flaw during build on Darwin, which in turn affects IBM Storage Copy Data Management. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Copy Data Management 2.2.0.0 - 2.2.23.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7154709

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	VPN TunnelVision Vulnerability (CVE-2024-3661)
Description	F5 has released workarounds addressing a VPN TunnelVision Vulnerability that exists in BIG-IP Access Policy Manager. **CVE-2024-3661** - By design, the DHCP protocol does not authenticate messages, including for example the classless static route option (121). An attacker with the ability to send DHCP messages can manipulate routes to redirect VPN traffic, allowing the attacker to read, disrupt, or possibly modify network traffic that was expected to be protected by the VPN. Many, if not most VPN systems based on IP routing are susceptible to such attacks. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (APM) versions • 17.1.0 - 17.1.1 • 16.1.0 - 16.1.4 • 15.1.0 - 15.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000139553

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-24788, CVE-2022-38096, CVE-2023-51042, CVE-2023-38545, CVE-2023-38546, CVE-2023-28322, CVE-2023-28320, CVE-2023-28319, CVE-2023-28321, CVE-2023-6546, CVE-2024-0565, CVE-2023-6931, CVE-2024-1086, CVE-2023-46219, CVE-2023-46218, CVE-2023-45288, CVE-2023-46120)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Storage Copy Data Management. These vulnerabilities could be exploited to cause Denial of service, Privilege escalation, Heap based buffer overflow, Security restriction bypass. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Copy Data Management 2.2.0.0 - 2.2.23.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7154709 • https://www.ibm.com/support/pages/node/7154710 • https://www.ibm.com/support/pages/node/7154711

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20404, CVE-2024-20405)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in Cisco Finesse Web-Based Management Interface. **CVE-2024-20404** - Due to insufficient validation of user-supplied input for specific HTTP requests that are sent to an affected system, an unauthenticated-remote attacker could conduct an SSRF attack on an affected system. **CVE-2024-20405** - Due to insufficient validation of user-supplied input for specific HTTP requests that are sent to an affected device, an unauthenticated-remote attacker could conduct a stored XSS attack by exploiting an RFI vulnerability. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Finesse Release • 11.6(1) ES11 and earlier • 12.6(2) ES01 and earlier Cisco Unified Contact Center Express Release • 12.0 and earlier • 12.5(1) SU3 ES05 and earlier The following Cisco products that may be bundled with Cisco Finesse are also affected • Packaged Contact Center Enterprise (Packaged CCE) • Unified Contact Center Enterprise (Unified CCE) • Unified Contact Center Express (Unified CCX) • Unified Intelligence Center
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-ssrf-rfi-Um7wT8Ew

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.